**Before the**
**FEDERAL EMERGENCY MANAGEMENT AGENCY**
**Washington, D.C. 20472**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Voluntary Private Sector Accreditation and<br>Certification Preparedness Program | )<br>) | Docket ID FEMA-2008-0017 |

---

## COMMENTS OF ASIS INTERNATIONAL

ASIS International (ASIS) submits these comments in response to the Federal Register Public Notice released December 24, 2008, in the above referenced docket. ASIS is the largest organization for security professionals, with more than 36,000 members worldwide. ASIS members are closely involved in overseeing and executing security and preparedness plans at all types and sizes of businesses. Drawing upon the first-hand expertise of its members, as well as working with other experts and organizations in the field, ASIS has worked for decades to develop ways for companies and organizations to be become better prepared and resilient.

ASIS is encouraged by discussions and pronouncements by DHS that for the private sector to adequately and voluntarily establish preparedness programs, it should be given the flexibility to choose from various standards, that best meet their needs for preparedness. As one of the co-authors of the Sloan Report on Title IX of H.R. 1 "Framework for Voluntary Preparedness", we would like to re-emphasize the primary recommendation of this document:

> *"For the private sector to adequately and voluntarily establish preparedness programs, it should be given the flexibility to choose from various standards, guidelines and best practices that best meet the respective organization's needs for preparedness. Organizations that have implemented preparedness management controls, best practices or complementary systems which address the core elements should be recognized and "credited" as demonstrating preparedness. Regulated industries should be given credit for their compliance with relevant regulations without the need for duplicative systems."*

ASIS is an American National Standards Institute (ANSI) Accredited Standards Development Organization (SDO). In its capacity as an SDO, ASIS has spearheaded the development of a new American National Standard entitled "Organizational Resilience: Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use". It is in the final stages of development and ratification, the Standard is a response to requests of ASIS members worldwide for a comprehensive standard for security, preparedness and business continuity to better prevent, avoid, prepare for, respond to and recover from disruptive incidents. The standard also addresses the Proposed Target Criteria for a Comprehensive Preparedness Standard outlined by DHS. (See chart in Attachment 1).

This standard is unique in that is takes a comprehensive ISO management systems approach for security, preparedness, response, mitigation, business/operational continuity and recovery for disruptive incidents resulting in an emergency, crisis, or disaster. By utilizing the ISO management system approach, not only can it be readily implemented by organizations using other ISO standards, but it can be cost-effectively audited and certified to by an auditing process that is compatible and consistent with the clearly understood methodology of existing ISO standards. Third party certification is an integral component of the Voluntary Private Sector Accreditation and Certification Preparedness Program (PS-Prep), and some other leading comprehensive preparedness standards by their own admission are not compatible with third party certification.

ASIS believes it is critical that this standard be adopted by DHS and included in the choices of standards in the PS-Prep program.

The Organizational Resilience standard is distinctive, complements and improves upon existing standards addressing business continuity (BCM) and emergency management (EM) by way of:

1. Focusing on the holistic resiliency of the organization not just BCM and EM. The standard emphasizes a balance of proactive and reactive strategies for making organizations resilient based on their risk profile and business environment in which they operation.
2. It is business friendly in that it uses the globally tested and proven ISO management systems approach. Therefore, this Standard is aligned with ISO 9001:2000, ISO 14001:2004, ISO/IEC 27001:2005, and ISO 28000:2007 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards.
3. The ISO approach (as used in this standard) is globally accepted and widely implemented. Therefore, American businesses involved in international business will be positioned to segway into the ISO standard based on this standard that is being proposed as a new work item proposal in ISO.
4. Compliance with this Standard can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001:2000, ISO 14001:2004, and/or ISO/IEC 27001:2005, and the PDCA Model. Therefore, there is no need to reinvent the wheel.
5. This standard, by taking a multi-disciplinary approach, is aligned with the way successful businesses manage risk by looking at the entire risk profile and not siloing risks.
6. This standard, using the ISO management systems approach, addresses the Proposed Target Criteria for Preparedness Standard (see attached mapping**)** of the standard with the DHS criteria – the section in the ASIS document addressing the subject area is embedded in the table).

As a complement to this standard, ASIS with the British Standards Institute has launched a joint development standard initiative for an American National Standard on BCM. The new standard will use the ISO management systems approach and be based on BSI's BS 25999 standard (Part 1 – Code of Practice; Part 2 – Specification). It will provide a unified approach to BCM on both sides of the Atlantic, effectively eliminating marketplace confusion and providing a model for the future ISO BCM standard. With the planned reciprocation between the standards, US companies can begin building their BCM programs immediately by using the already mature BS25999 framework. The new American National Standard will allow domestic as well as international certification.

Therefore, ASIS believes it is critical that the BS25999-1 and the American National Standard on BCM be included in the choices of standards under the Voluntary Private Sector Accreditation and Certification Preparedness Program. It should be noted that this American National Standard initiative to develop a BCM standard that is both auditable and scalable (and addresses the most of the core DHS criteria) has a technical committee of approximately 150 BCM experts from around the globe including representatives from Disaster Recovery Institute International, Association of Contingency

Planners, the Business Continuity Institute and its U.S. Chapter BCI-USA, some of the major BCM associations.

In closing, we would also like re-emphasize another important recommendation of the Sloan Report, where a lack of knowledge and experience was identified as the key barrier to improved resilience in the private sector:

> *"The next effort should concentrate on creating tools to evaluate existing programs, and developing training materials, case studies, tool sets, technical assistance and peer programs to assist small and medium businesses develop and enhance their preparedness programs. The challenge is how to implement the above approaches in a cost-effective fashion. For the private sector to improve preparedness performance, it needs the tools and knowledge how to address the core elements in a business sensible fashion. Much can be learned from the decades of experience in quality and environmental management, particularly tailoring approaches that address the needs of small and medium businesses."*

**ATTACHMENT I**

| | Proposed Target Criteria for Current Standard Selection | | | Examples of Desired Content for Comprehensive Preparedness Standard Criteria | |
|---|---|---|---|---|---|
| | Subject Area | ASIS Standard – Organizational Resilience | Critical Elements and Content | ASIS Standard Organizational Resilience Management | |
| 1 | Scope and Policy | 4.1 4.2<br>A.1 A.2<br>4.1.1 A.1<br>4.2.1 A.2<br>4.2.2 A.2.2<br>4.2.2 A.2.2 | A scope and/or policy statement that addresses disaster/emergency management, business continuity management, and organizational resilience. We recommend that the standard contain the following:<br>1. Scope.<br>2. Policy.<br>3. Principles.<br>4. Purpose. | 4.1.1 A.1<br>4.1.1 A.1<br>4.2.1 A.2<br>4.2.2 A.2 | 1. Establish the project to address preparedness management including provision of appropriate resources and authorities for conduct of project.<br>2. Define scope and boundaries for development and implementation of the preparedness management program.<br>3. Establish a policy to provide a framework for setting objectives and provide the direction and principles for action.<br>4. Demonstrate top management and the organization's commitment to meeting the requirements of preparedness management. |
| 2 | Requirements | 4.3.2 A.3.2<br>4.3.2 A.3.2<br>4.3.2 A.3.2<br>4.3.2 A.3.2 | A requirement that acknowledges or otherwise directs the organization to identify and conform to applicable legal, statutory, regulatory and other requirements (e.g., codes of practice and standards of care). We recommend that the standard contain and incorporate the following, and ensure a process for identifying and addressing them:<br>1. Legal.<br>2. Statutory.<br>3. Regulatory.<br>4. Other. | 4.3.2 A.3.2<br>4.3.2 A.3.2<br>4.3.1 A.3.1 | 1. Identify legal and other requirements which govern the organization's activity.<br>2. Establish a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the organization's functions, activities and operations.<br>3. Understand potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to the location and industry. |
| 3 | Objectives and Strategies | 4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.5.3 A.5.3 | A requirement that sets objectives and strategies. We recommend that the standard set or establish requirements for strategies and/or strategic plans designed to accomplish the organization's objectives in:<br>1. Risk Management.<br>2. Incident Prevention.<br>3. Incident Preparedness.<br>4. Incident Mitigation.<br>5. Incident Response.<br>6. Business Continuity.<br>7. Incident Recovery.<br>8. Corrective and Preventive Actions. | 4.3.3 A.3.3<br>4.4.1 A.4.1<br>4.4.1 A.4.1<br>4.4.6 A.4.6<br>4.4.7 A.4.7<br>4.3.3 A.3.3<br>4.3.3 A.3.3<br>4.3.1 A.3.1<br>4.4.3 A.4.3 | 1. Develop strategic plans for incident prevention, preparedness, mitigation, response, business continuity, system resiliency, and recovery for short term (less than a month) and long term (up to one year).<br>2. Identify type and availability of human, infrastructure, processing, and financial resources needed to achieve the organization's objectives.<br>3. Identify roles, responsibilities, authorities and their interrelationships within the organization required to ensure effective and efficient operations.<br>4. Plan the operational processes for actions required to achieve the organization's objectives.<br>5. Include cyber and human security elements in control strategies and plans.<br>6. Make arrangements (e.g., Memoranda of Agreements) and contingency preparedness plans that need to be in place to manage foreseeable emergencies.<br>7. Develop Crisis Communication Plans with internal personnel (management, staff, response teams, etc.). |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 4.4.3 A.4.3<br>A.4.4.7<br>A.5.2.2 | 8. Ensure the company's Communications Department has identified key resources designated to initiate crisis communications with employees, business partners, vendors, government and external media.<br>9. Involve appropriate external parties during exercise events. |
| 4 | Risk Management | 4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1 | A requirement for risk management to include hazard and threat identification, risk assessment, vulnerability analysis, and consequence / business impact analysis. We recommend that the standard provide for the conduct of:<br>1. Hazards and Threats Identification.<br>2. Risk Assessment.<br>3. Impact Analysis.<br>4. Vulnerability Assessment.<br>5. Consequence / Business Impact Analysis. | 4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1<br>4.3.1 A.3.1 | 1. Establish a process for risk identification, analysis, and evaluation.<br>2. Identify assets, needs, requirements, and analysis of critical issues related to business disruption risks that are relevant to the organization and stakeholders.<br>3. Identify hazards and threats, to include cyber and human security elements. These should include loss of IT; telecommunications; key skills; negative publicity; employee or customer health or safety; damage to organization's reputation; loss of access to organization's assets; utility systems; supply chain outage/disruption, and insider threats.<br>4. Evaluate the probability of a disruptive event, dependencies and interdependencies with other assets and sectors, and consequences on business operations Prioritize the issues identified as a result of the risk assessment and impact analysis.<br>5. Set objectives and targets (including time frames) based on the prioritization of issues within the context of an organization's policy and mission.<br>6. Evaluate and establish recovery time objectives.<br>7. Assess vulnerability of organization, systems, and processes.<br>8. Define risk treatment strategy and resources needed to address the organization's risks to business disruption. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Operations, Control, and Risk Mitigation | 4.4 A4<br>4.4.6 A.4.6<br>4.4.7 A.4.7<br>A.4.2 A.4.3 | Requirements for the organization's incident management / business continuity strategy, tactics, operational plans and procedures, and/or contingency plans that will be used during emergencies, crises and other events threatening its operation; and the documentation thereof. We recommend that the standard contain provisions for the following:<br>1. Operational Continuity.<br>2. Incident Management.<br>3. Coordination with Public Authorities. | 4.4.6 A.4.6<br>4.4.7 A.4.7<br>4.4.7 A.4.7<br>4.4.6 A.4.6<br>4.4.6 A.4.6<br>4.4.4 A.4.4<br>4.4.5 A.4.5<br>4.4.6 A.4.6 | 1. Establish operational control measures needed to implement the strategic plan(s) and maintain control of activities and functions against defined targets.<br>2. Develop procedures for controlling key activities, functions, and operations associated with the organization, including possible large extended workforce absences; and alternative work sites or remote working procedures.<br>3. Establish processes and procedures for operational management and maintenance of infrastructure, plant, facilities, finance, etc. which have an impact on the organization's performance and its stakeholders.<br>4. Establish processes and procedures for management of documents which are essential to the successful implementation and operation of the preparedness management program or system.<br>5. Establish operational control measures needed to implement the strategic plan(s) and maintain control of |

| | | | | | |
|---|---|---|---|---|---|
| | | | | <br>4.4 A.4<br>4.4 A.4<br>4.4.6 A.4.6<br>4.4.7 A.4.7<br>4.4.7 A.4.7<br>4.4.7 A.4.7<br>4.4.4 A.4.4<br>4.5.4 A.5.4<br>4.5.2 A.5.2<br>A.4.2 A.4.3<br>4.4.7 A.4.7 | activities and functions.<br>6. Develop insider threat mitigation measures.<br>7. Develop action plans for increased threat levels and tools to enhance situational awareness.<br>8. Formalize arrangements for those who supply and contract their services to the organization which have an impact on the organization's performance, including mutual aid agreements.<br>9. Determine the local and regional public authorities and their potential impact on your organization's plans including, but not limited to, the U.S. Department of Homeland Security, emergency management, fire, police, public utilities, and local & nationally elected public officials.<br>10. Work with local Public Information Officers to understand and follow protocol.<br>11. Document the forms and processes to be used before or during an event or exercise to ensure activities and participants, etc., are captured for review and Plan response and recovery improvements.<br>12. Collaborate with other organizations on preparedness issues of mutual concern. |
| 6 | Communications | <br>4.4.3 A.4.3<br>4.4.3 A.4.3<br>4.4.3 A.4.3<br>4.4.3<br>A.4.3 | Requirements for communication and warning as they apply to disaster/emergency management and business continuity. We recommend that the standard contain provisions for the following:<br>1. Warning and Notification.<br>2. Event Communication.<br>3. Crisis Management Communications.<br>4. Information Sharing.<br>5. Public Relations. | 4.4.3 A.4.3<br>4.4.3 A.4.3<br>4.4.3 A.4.3<br>4.4.3 A.4.3<br>4.4.3 A.4.3<br>4.4.3 A.4.3 | 1. Develop and maintain a system required for communications and warning capability in the event of an incident / disruption.<br>2. Identify requirements, messages, and content required for communication within the organization.<br>3. Identify requirements, messages, and content required for external communication.<br>4. Develop, coordinate, evaluate and exercise plans to communicate information and warnings with internal stakeholders and external stakeholders (including the media) for normal and abnormal conditions.<br>5. Make arrangements for communications both within the organization and to/from external sources, including local, state and federal law enforcement and first responder organizations.<br>6. Document procedures and identify tools to manage relationships and communications processes with external partners: business partners, governmental agencies, vendors, etc. |
| 7 | Competence and Training | <br>4.4.2 A.4.2<br>4.4.2 A.4.2 | Requirements for the competence / qualifications and training of organization's personnel, contractors, and other relevant stakeholders involved in emergency management and business continuity management. We recommend that the standard contain provisions for the following:<br>1. Competence.<br>2. Training. | 4.4.2 A.4.2<br>4.4.2 A.4.2<br>4.4.2 A.4.2 | 1. Assess, develop and implement training/education program(s) for the organization's personnel, contractors, and other relevant stakeholders.<br>2. Identify and establish skills, competency requirements, and qualifications needed by the organization to maintain operations.<br>3. Develop organizational awareness and establish a culture to support emergency / disaster preparedness |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 4.4.1 A.4.1<br>4.4.2 A.4.2 | and business continuity management.<br>4. Determine organizational interface protocol, identification and training requirements and assign appropriate internal staff or support representative(s). |
| 8 | Resource Management | 4.4.1 A.4.1<br>4.4.1 A.4.1<br>4.4.7 A.4.7 | Requirements for resources management and/or logistics as it relates to the allocation of human, physical, and financial resources in the event of incidents/emergencies that threaten operations We recommend that the standard contain provisions for the following:<br>1. Resource Management.<br>2. Logistics and Business Processes. | 4.4.1 A.4.1<br>4.4.1 A.4.1<br>4.4.7 A.4.7<br>4.4.1 A.4.1<br>4.4.7 A.4.7 | 1. Identify and assure availability of human, infrastructure, and financial resources in the event of a disruption.<br>2. Establish and document provisions for adequate finance and administrative resources and procedures to support the management program or system under normal and abnormal conditions.<br>3. Make arrangements for mutual aid and community assistance. |
| 9 | Assessment and Evaluation | 4.5 A.5 | Requirements for assessments, audits and/or evaluation of disaster / emergency management and business continuity programs. We recommend that the standard contain provisions for Periodic Assessment and Performance Evaluation. | 4.5.1 A.5.1<br>4.5.3 A.5.3<br>4.5.5 A.5.5<br>4.5.2.2 A.5.2.2<br>4.6 A.6<br>4.6 A.6 | 1. Establish metrics and mechanisms by which the organization assesses its ability to achieve the program's goals and objectives on an ongoing basis.<br>2. Determine nonconformities and the manner in which these are dealt with.<br>3. Conduct internal audits of system or programs.<br>4. Plan, coordinate, and conduct tests or exercises.<br>5. Evaluate and document exercise results.<br>6. Review exercise results with management to ensure corrective action is taken.<br>7. Report audits and verification results to chief executive officer. |
| 10 | Continuing Review (ongoing management and maintenance) | 4.6.2 4.6.3 A.6.2 A.6.3<br>4.6.4 A.6.4<br>4.6.5 A.6.5 | Requirements for program revision and process improvement including correction actions. We recommend that the standard contain provisions for the following:<br>1. Review.<br>2. Maintenance.<br>3. Process improvement. | 4.6 A.6<br>4.6 A.6 | 1. Conduct management review of programs and/or system to determine its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary.<br>2. Make provisions for improvement of programs, systems, and/or operational processes. |